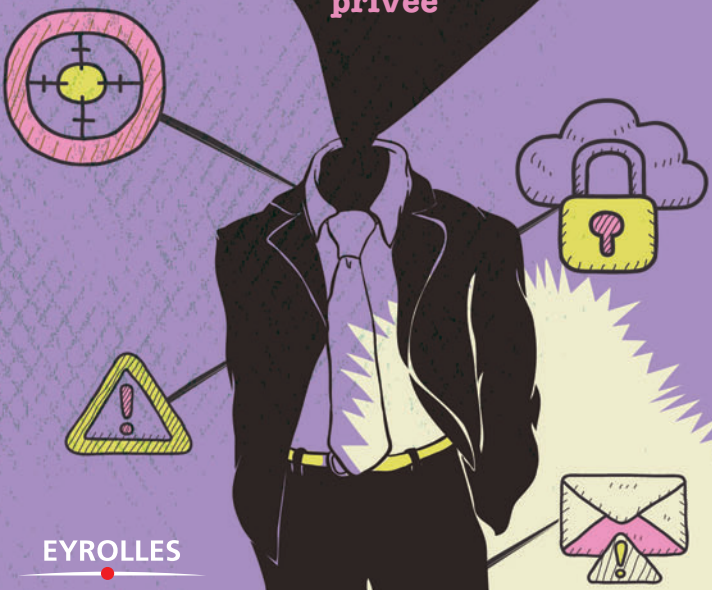
Connectez-moi !

Martin Untersinger

Préface de Benjamin Bayart

ANONYMAT sur INTERNET

Comprendre pour protéger sa vie privée



EYROLLES

 ISBN : 978-2-212-13500-8

Préface

C'est devenu une banalité, fausse, que de dire qu'Internet est en train de changer nos sociétés. Sauf à lui supposer une origine divine, Internet n'a pas été imposé à la société depuis l'extérieur ni n'est en train de la réformer contre son gré. Internet est l'outil dont les sociétés humaines occidentales se sont dotées pour évoluer, pour changer. Ce changement prend bien des formes, et touche bien des aspects, dont les mieux compris et analysés touchent à l'échange de biens immatériels et à la liberté d'expression.

Concernant l'échange des biens immatériels, par exemple le partage de fichiers musicaux ou de vidéo, la caricature du vol souvent employée n'a pas de sens, puisque l'ancien exemplaire du fichier est *toujours* sur le disque dur où il se trouvait auparavant. Si le fait de regarder la baguette de pain dans la vitrine en fait apparaître, magiquement, une nouvelle dans ma main, je ne vole pas le boulanger. Cet échange de biens immatériels a des conséquences sur les modèles économiques de nombreuses industries, à commencer par celle du divertissement. Quand on fait métier de vendre des copies sur support plastique, comment survivre à l'apparition de la fantastique machine à copier qu'est Internet ?

Quant à la liberté d'expression, c'est simplement le fait que chaque citoyen puisse s'exprimer publiquement, et ait l'opportunité d'être lu et entendu par tous. Au siècle dernier, protéger la liberté d'expression, c'était protéger la liberté de la presse. La seule forme d'expression accessible au commun était alors la discussion autour de la table au dîner de Noël, ou au café du coin. Ce qui était, au siècle dernier, réservé à une minorité (journa-

listes, artistes, dirigeants divers, etc.) est maintenant accessible à tous. Quiconque a un mur Facebook, un blog, un compte Twitter, un tumblr, dispose d'un lieu d'expression qu'il peut ouvrir au public. Sur Internet, tout le monde est éditeur de ce qu'il publie, tout le monde est éditorialiste et chroniqueur. La question des libertés, et des règles de société, qui vont avec cette expression publique, est une question majeure de l'organisation des sociétés post-Internet, une question politique : comment voulons-nous faire société ensemble ?

Cette question se décline en de nombreuses facettes. À commencer par celle du pouvoir qu'ont certains intermédiaires techniques sur notre vie numérique. Tout ce que je dis et fais sur Internet passe par mon fournisseur d'accès. Quel pouvoir de censure a-t-il ? Quel pouvoir d'intrusion a-t-il ?

C'est une des premières questions que je me suis posées sur le sujet, il y a plus de 15 ans. J'y ai répondu en ayant un accès Internet dans une association loi 1901, FDN, ce qui à l'époque était classique. J'y ai répondu en reprenant la présidence de l'association pour qu'elle ne disparaisse pas, pour que l'accès à Internet ne soit pas forcément une marchandise, et qu'il continue de pouvoir être autre chose qu'une marchandise. Et en étant toujours, en 2013, dix-sept ans plus tard, abonné d'un fournisseur d'accès associatif.

Les intermédiaires techniques sont nombreux à avoir un fort pouvoir de nuisance dans le monde numérique. Outre le fournisseur d'accès, il y a également le fournisseur de l'ordinateur (que ce dernier ait la forme d'un téléphone n'y change rien), ou le fournisseur de logiciel. Ces questions-là sont anciennes également. Pour ma part, j'ai fait le choix évident du logiciel libre précisément pour ces raisons : *mon* ordinateur fait ce que *je* veux, plutôt que ce qu'un éditeur a choisi qu'il fasse pour des raisons qui ne sont pas les miennes.

Les grandes plates-formes de services sont finalement d'apparition plus récente, au milieu des années 2000. Mais leur place

au cœur de l'expression publique de chacun devient centrale et donc dangereuse. Là aussi, la question qui revient est toujours la même : qui est capable de décider, qui peut censurer, qui rend des comptes ? Au final, est-ce moi qui suis libre de m'exprimer, ou est-ce Twitter qui tolère ce que je dis aussi longtemps que ça l'arrange ?

Enfin, il y a la question de l'identité, encore mal comprise. Pourtant, les personnes qui s'expriment publiquement ont toujours pu le faire sous une identité qu'ils ont choisie, sculptée, choisissant le nom, mais aussi la personnalité qu'ils montrent au public. Pour preuve l'exemple simple de Johnny Hallyday, dont tout le monde se fiche de savoir qu'il s'appelle J.-P. Smet. Et ce n'est pas un privilège d'artiste. On peut également se faire élire président de la République sous un pseudonyme, comme ce fut le cas de Nicolas Sarközy de Nagy-Bocsa, élu sous le nom de Nicolas Sarkozy, sans tréma ni particule. Même le président des États-Unis est connu dans le monde entier sous le nom de Bill Clinton, alors que son prénom est William. Jusqu'au Pape, qui règne sous un faux nom.

Lorsqu'on prend la parole en public, on choisit le nom sous lequel on apparaît. Cette identité-là n'est pas forcément celle de l'état-civil, mais c'en est bien une. Qui, d'ailleurs, ne connaît quelqu'un dont le prénom dans la vie courante diffère de ceux inscrits sur sa carte d'identité, ou n'est pas le premier de ceux-là, ou encore n'est pas orthographié de même ?

Les identités sous lesquelles on souhaite apparaître peuvent être multiples, et pour de multiples raisons. On peut par exemple ne pas avoir le même nom dans un réseau militant (Chaban) et dans le monde politique (Delmas). Le choix de l'identité sous laquelle chacun s'exprime, en fonction du lieu et du contexte, relève des libertés attenantes à la liberté d'expression. Et ce droit relève, forcément, du droit de s'exprimer sans donner de nom, du droit à l'anonymat.

La question des identités, à l'heure du numérique et donc de la surveillance généralisée, est une question politique clé, une question majeure sur la façon dont nous voulons faire société. J'en prend un exemple simple : l'Assemblée Générale qui m'a élu président du Fonds de Défense de la Neutralité du Net l'a fait sans voir mes papiers d'identité. C'est l'individu qui s'exprime dans l'espace public sous le nom de Benjamin Bayart, reconnaissable à sa barbe et à ses cravates ridicules, qui a été élu à ce poste. Pourtant, c'est à la carte d'identité que le banquier a accordé la signature sur un compte bancaire. D'une certaine façon, le banquier n'a pas respecté le vote de l'Assemblée Générale, pourtant souveraine sur la question. Il a supposé que le Benjamin Bayart de l'état-civil était le même que celui de l'espace public.

Une forme numérique assez simple est pourtant au point depuis vingt ans : ma clef de chiffrement publique, qui est... publique. L'Assemblée Générale aurait pu élire comme président « la personne qui s'exprime avec cette signature », et le banquier aurait pu contrôler cette information, bien plus fiable que ce que raconte le support de plastique distribué par l'État. Ainsi il m'appartient de savoir et de faire savoir qui je suis, il m'appartient de me nommer, et l'état-civil ne sert qu'à enregistrer celui de mes noms qui servira dans mes échanges avec l'administration, ou lors du prochain recensement.

Les questions autour des identités, autour de l'anonymat qui en est le corollaire immédiat, autour du droit de ne pas être surveillé, autour du droit à la vie privée, sont des questions majeures pour comprendre la société qui est en train de se construire avec Internet. Et c'est une des questions qui restent le plus mal connues, même des spécialistes.

Benjamin Bayart
Président de la fédération FDN
(Fournisseurs d'accès à Internet associatifs)

Table des matières

Avant-propos

L'anonymat sur Internet souffre d'un paradoxe étrange. Alors qu'on utilise de plus en plus Internet, qu'on y laisse toujours plus de données et qu'il est de plus en plus facile de savoir qui y fait quoi, l'inquiétude quant à l'utilisation de ces données grandit chaque jour.

Pourquoi ce livre ?

Jamais anonymat et vie privée n'ont été à ce point discutés et débattus. Et pour cause, sur l'Internet d'aujourd'hui, l'asymétrie d'information est totale : si on voit bien les usages qu'on peut tirer de services gratuits « offerts » par Google et Facebook (ou autres sites financés par la publicité), ces derniers savent très bien que nos informations personnelles sont à la source de leur « création » de richesse.

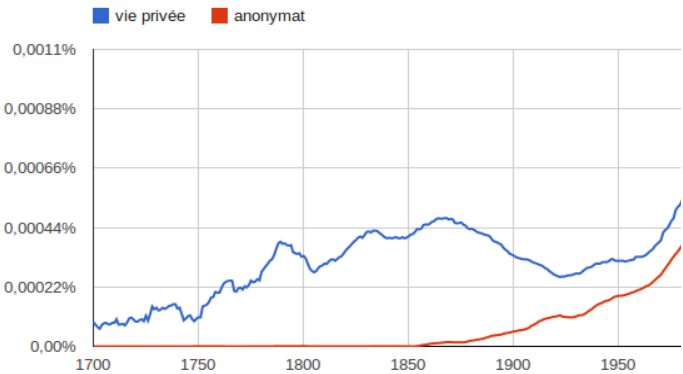


Fig. 0–1 > L'évolution des termes « vie privée » et « anonymat » dans le corpus de livres indexés par Google

L'internaute non averti, lui, ne sait absolument pas quel type d'information personnelle il donne, quand il la donne, pour combien de temps, dans quel but ou pour quel profit, ni même, parfois, qui la collecte.

Chiffres L'humanité, ou presque, sur Internet

À l'heure où nous écrivons ces lignes, il y a un demi-milliard d'utilisateurs sur Twitter[1], un milliard sur Facebook[2] et près de 200 millions de blogs[3] ; on n'a jamais autant parlé de soi sur Internet. Pour autant, la vie privée et l'anonymat n'ont jamais été aussi importants pour les internautes, à rebours d'un discours ambiant banalisant le naturisme numérique.

Sur un réseau dont la mémoire et les capacités de copie sont en théorie illimitées, nul ne sait ce que nous prépare l'accumulation de données, traces et autres informations personnelles que nous laissons par térabits entiers, quotidiennement, sur Internet.

EN SAVOIR PLUS **L'hypermnésie**

Vous pouvez consulter à ce sujet la section consacrée à l'hypermnésie, du manuel *Informatique et sciences du numérique.*

🕮 *Informatique et sciences du numérique*, Gilles Dowek *et al.*, Eyrolles, 2012.

Une véritable option d'informatique a enfin fait son entrée au lycée, à quoi répond ce manuel adressé aux lycéens de Terminale S ayant choisi la spécialité ISN. C'est un manuel que chacun peut (et devrait) lire – en tout cas tout lecteur souhaitant comprendre les bases de l'informatique.

C'est sans compter les utilisateurs situés dans des pays intolérants, prompts à la censure ou à l'intimidation, et les citoyens occidentaux, parfois effrayés par les velléités étatiques de contrôle et d'identification sur les réseaux et par les divers systèmes de traçabilité installés par les entreprises ou les particuliers.

Internet a beau être un média pensé et fait pour mener une vie publique, le glissement sur les réseaux de nos existences, de nos secrets et de notre intimité fournit de multiples raisons de protéger son anonymat et, de fait, son identité et sa vie privée.

Ce livre va tenter de vous donner une palette d'outils, de l'astuce la plus simple à la stratégie la plus complexe, pour comprendre et protéger les informations que vous laissez filer à chacune de vos connexions.

DÉFINITIONS **Anonymat, vie privée, identité, sécurité…**

Des thèmes connexes à l'anonymat seront évoqués et traités dans ce qui va suivre : vie privée, sécurité informatique… Il était difficile de faire autrement, tant ces domaines sont liés. Nous espérons, avec ce livre, faire un pont entre la théorie et la pratique, comprendre les mouvements en marche sur Internet pour mieux y adapter sa stratégie, comprendre le pourquoi pour appliquer le comment.

Sur Internet, « on ne peut pas ne pas laisser de traces[4]. » Pourtant, ces outils sont nécessaires à ceux que cette bataille interpelle, intéresse ou inquiète. Entre les grandes entreprises américaines qui tentent par tous les moyens de faire changer la perception de ce qui peut être privé et public sur le réseau, la peur bleue des gouvernements de ce qui se passe sur Internet et les initiatives individuelles ou émanant d'entreprises qui se vantent de toujours davantage protéger la vie privée des internautes, les lignes de démarcation sont floues et mouvantes. Nous espérons modestement vous donner quelques points de repères au fil de ces pages.

Quant aux protections et aux outils que nous aborderons, ils sont parfois difficiles à comprendre et à appliquer : les menaces sur votre identité sont multiples, et chacune présente ses caractéristiques propres. La sécurité est une question compliquée que l'on ne peut résoudre qu'en s'armant de temps, de patience et d'envie. Même si l'anonymat absolu n'existe pas, cela ne veut pas dire qu'il faut abandonner toute volonté de protection.

L'habitude est l'ennemie de la sécurité. Appliquer bêtement des processus et utiliser des logiciels sans comprendre leur fonctionnement peut tout autant vous mettre en danger que vous protéger. La sécurité informatique est un ensemble cohérent où tout se tient. Les processus et les réflexes qui lui sont associés changent en permanence selon les évolutions technologiques, étatiques, juridiques ou commerciales. La sécurité n'est jamais acquise. C'est pourquoi ce livre ne donnera pas une liste exhaustive et définitive des moyens de protéger son anonymat et sa vie privée.

Péremption **La technique évolue (vite)**

Dans le champ de la sécurité informatique, rien n'est jamais vraiment acquis. Certaines des solutions abordées dans cet ouvrage peuvent être obsolètes au moment de votre lecture, même si nous avons fait tout notre possible pour aborder uniquement des solutions éprouvées.

Plan de l'ouvrage

Après avoir défini un certain nombre de termes et rappelé quelques principes du fonctionnement d'Internet concernant l'anonymat (**chapitre 1**), on démontrera que l'anonymat total n'existe pas (**chapitre 2**). Pour autant, les raisons pour camoufler ses traces et son identité sont nombreuses (**chapitre 3**). Après avoir abordé les bases de la protection (**chapitre 4**), on se penchera sur les stratégies à mettre en place pour contourner la surveillance des entreprises et des géants du Web (**chapitre 5**). Puis on apprendra à protéger ses communications, notamment ses e-mails et ses discussions instantanées (**chapitre 6**), avant de se pencher sur la protection de sa connexion (**chapitre 7**) et d'aborder quelques outils plus techniques pour ceux qui désireraient aller plus loin (**chapitre 8**). Avant de dresser quelques pistes sur l'avenir de l'anonymat et de la vie privée sur Internet (**chapitre 10**), on abordera les réflexes fondamentaux à adopter sans même installer le moindre logiciel (**chapitre 9**).

Remerciements

Cet ouvrage n'aurait jamais vu le jour sans le premier modem, arrivé dans la maison familiale à la fin des années 1990, et sans Muriel Shan Sei Fan et son e-mail de février 2012.

Je tiens également à remercier Chloé, qui aura supporté de m'entendre déblatérer des heures durant sur la vie privée et la cryptographie pendant des mois en faisant mine de s'y intéresser (et pour le reste aussi). Il me faut également remercier l'équipe de Rue89, et plus particulièrement mes rédacteurs en chef, dont la confiance et la liberté qu'ils m'ont accordées sont pour beaucoup dans la réalisation de cet ouvrage, ainsi que les fidèles acolytes que sont Pirhoo, Mayeu et Pierre Alonso, pour leur aide et leurs relectures précieuses. Merci aussi aux

tenanciers et piliers de bars de la mailing-list « AH » (ils se reconnaîtront) pour leur humour, leurs gifs animés et leurs sarcasmes, précieux alliés des derniers jours de rédaction. Les internautes qui ont gentiment répondu à mes questions sur les réseaux sociaux doivent aussi être remerciés ici, dont (j'en oublie) : @lactualaloupe, @_swayb, @nkgl, @barzin, @bmalynovytch, @zefede, @Zizounnette, @_LilyRUsh, @johanhufnagel ou encore @szadkowski_m. Enfin, sans les innombrables internautes, activistes, hackers et autres passionnés plus ou moins anonymes, qui ont passé du temps et de l'énergie à alimenter les ressources indispensables que sont *free.korben.info*, le site de l'EFF, les diverses publications du collectif Tactical Tech, le Cryptoparty Handbook, cet ouvrage ne serait pas ce qu'il est. Merci à eux.

Index

R

S

T